Telecommunications Standards Advisory Committee (TSAC)

Reference Specification

Secure Deployment of Quantum Key Distribution Networks

Draft IMDA RS SecQKDN
Issue 1, February 2026

Info-communications Media Development Authority
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Acknowledgement

The Info-communications Media Development Authority (IMDA) and the Telecommunications Standards Advisory Committee (TSAC) would like to acknowledge the following members of the TSAC Focus Area (FA) 7 Secure Deployment of Quantum Key Distribution Networks Task Force (TF) for their invaluable contributions to the preparation of this Reference Specification:

Draft IMDA RS SecQKDN, Issue 1, February 2026	Reference Specification for Secure Deployment of Quantum Key Distribution Networks
Focus Area 7 Chairperson	Dr Lim Woo Lip, Senior Vice President/Chief Technology Officer, Cyber, Singapore Technologies Engineering Ltd
Secure Deployment of Quantum Key Distribution Networks Task Force Chairperson	Mr Heng Kwee Tong, Head, Engineering & Corporate IT, SPTel Pte. Ltd. Mr Kenneth Hwang, Vice President, Client Solutions & Transformation, Singapore Telecommunications Limited
Editors	Mr Yong Hai Hung, Director IP & Transport Engineering, SPTel Pte. Ltd. Mr Dennis Lam, Director, Enterprise Architects, Singapore Telecommunications Limited Dr Hao Qin, Senior Research Fellow, Centre for Quantum Technologies - National University of Singapore Dr Haw Jing Yan, Senior Research Fellow, Centre for Quantum Technologies - National University of Singapore Mr Nicolas Pouymonbrat, Lead Consultant, Quantum Solutions, ID Quantique
Secretary	Ms Kong Pei Wee, Senior Manager, Info-communications Media Development Authority

List of TSAC FA 7 Secure Deployment of Quantum Key Distribution Networks Task Force Members (2025-2027)

S/N	Organisation	Name
1	Ciena Communications Singapore Pte. Ltd.	Mr Gideon Hoe, Senior Consultant
2	Ciena Communications Singapore Pte. Ltd.	Mr Rifaat Shekh-Yusef, Product Security Architect
3	CISCO Singapore	Mr William Yeo, Data Center Technical Solution Architect
4	Cyber Security Agency of Singapore	Mr Ching Weiwen, Senior Cybersecurity Consultant, CEC
5	Cyber Security Agency of Singapore	Mr Roddy Kok, Lead Cybersecurity Consultant, CEC
6	Defence Science and Technology Agency	Mr Too Huseh Tien, Deputy Director, Infocomm Digital Platforms
7	Fortinet Singapore Pte. Ltd.	Mr Yonathan Khor, Regional Cybersecurity Consultant
8	Fraunhofer Singapore Pte. Ltd.	Dr Michael Kasper, CEO
9	Government Technology Agency of Singapore	Mr Tan Peng Chong, Principal Cybersecurity Specialist
10	Huawei International Pte. Ltd.	Dr Li Zhengyu, Quantum Communication Researcher
11	Huawei International Pte. Ltd.	Mr Liu Yong Tai, Solution Director (Fixed Network)
12	Infocomm Media Development Authority	Mr Chua Chuen Hou, Director, Digital infrastructure Technologies
13	ID Quantique	Mr Jean-Robert Morax, Q-Safe Product Manager
14	Nokia Technology Pte. Ltd.	Mr Richard Tan, Head of Solution Business Development, South-East Asia
15	Nanyang Technological University	Associate Professor Anupam Chattopadhyay, , College of Computing and Data Science
16	Setsco-An Security Pte. Ltd.	Mr Samuel Mak, Security Analyst
17	SGS Testing & Control Services Singapore Pte. Ltd. (SGS Brightsight)	Mr Gavin Duan, Cybersecurity Lab Manager
18	Singapore Technologies Engineering Ltd.	Mr Huang Shiwei, Assistant Manager
19	Singapore Technologies Engineering Ltd.	Dr Amelia Tan, Head, Quantum Group Technology Office
20	Singapore Telecommunications Limited	Mr Maung Min Thein, Director, Engineering

21	SpeQtral Pte. Ltd.	Dr Alexander Dixon, Head of Quantum Projects
22	SpeQtral Pte. Ltd.	Mr Cyril Tan, Security Architect
23	Thales DIS (Singapore) Pte Ltd	Mr Nitesh Parasher, Senior Sales Engineer, Cyber Security Products
24	The Thought Projects Pte. Ltd.	Dr Lim Han Chuen, Director
25	Toshiba Asia Pacific Pte. Ltd.	Mr Anandaraman Sankaran, Senior Manager, QKD Technical Marketing
26	UL Solutions	Mr Chue Wai Lian, TS Team Leader (Identity Management and Security)
27	Utimaco IS Pte. Ltd.	Dr Volker Krummel, Technical Manager, Cryptography
28	Viavi Solutions Singapore Pte. Ltd.	Dr Tsunehiko Chiba, Head of APAC CTO Innovation Center
29	Viavi Solutions Singapore Pte. Ltd.	Mr Johnson Tay, Business Development Lead

Telecommunications Standards Advisory Committee (TSAC)

The TSAC advises IMDA on the setting of ICT standards as well as on the development and recommendation of specifications, standards, information, guidelines and other forms of documentation for adoption and advancement of the standardisation effort of the Singapore ICT industry (hereafter termed "IMDA Standards").

Telecommunications standards-setting in Singapore is achieved with the assistance of TSAC, where professional, trade and consumer interest in telecommunications standards is represented on the TSAC with representatives from network and service operators, equipment suppliers and manufacturers, academia and researchers, professional bodies and other government agencies.

List of TSAC Members (2024-2027)

TSAC Chairman:

Dr Chin Woon Hau	Director (Technology & Standards) Info-communications Media Development Authority

TSAC Members:

Mr George Choo	President, Association of Telecommunications Industry of Singapore
Mr Andy Phang	Assistant Director, Technology & Standards, Info-communications Media Development Authority
Mr Marcus Tan Cheng Lin	Head of Cybersecurity Department Institute for Infocomm Research
Mr Denis Seek	CTO M1 Limited
Mr Ng Thian Khoon	Head, Broadcast Engineering/ Broadcast Engineering (Technology) Mediacorp Pte. Ltd.
Associate Professor Chau Yuen	Associate Professor, School of Electrical & Electronic Engineering Provost's Chair in Wireless Communications Nanyang Technological University
Professor Biplab Sikdar	Professor, Head of Department, Electrical and Computer Engineering, & Area Director (Communications & Networks) National University of Singapore
Mr Gao Peng	Head of Radio Planning Simba Telecom Pte. Ltd.
Professor Susanto Rahardja	Professor, Engineering Cluster Singapore Institute of Technology
Mr Lim Yu Leong	Vice President, Group Strategy, Engineering & Innovation Singapore Telecommunications Limited
Professor Tony Quek	Head of Information Systems and Technology Design Pillar; Cheng Tsang Man Chair Professor Singapore University of Technology and Design
Mr Heng Kwee Tong	Head, Engineering & Corporate IT SPTel Pte. Ltd.
Mr Eddie Teo Soo Kwok	Assistant Vice President, Radio Technology StarHub Ltd.

This page is intentionally left blank.

Contents

This Reference Specification is a living document which is subject to review and revision.

Reference Specifications and Guides are informative documents and are not used for approval of customer equipment. They are either one of the following types of documents:

Informative and interim documents on customer equipment standards which are yet to be adopted by network operators; or

Informative documents describing network standards adopted by the public telecommunication networks in Singapore.

NOTICE

THE INFO-COMMUNICATIONS MEDIA DEVELOPMENT AUTHORITY ("IMDA") MAKES NO REPRESENTATION OR WARRANTY OF ANY KIND WITH REGARD TO THE MATERIAL PROVIDED HEREIN AND EXCLUDES ANY EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS OF NON-INFRINGEMENT, MERCHANTABILITY, SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE. SUBJECT TO THE MAXIMUM EXTENT PERMITTED UNDER LAW, IMDA SHALL NOT BE RESPONSIBLE OR LIABLE TO YOU OR ANY THIRD PARTY FOR ANY ERRORS AND/OR OMISSIONS CONTAINED HEREIN OR FOR ANY LOSSES OR DAMAGES (INCLUDING ANY LOSS OF PROFITS, BUSINESS, GOODWILL OR REPUTATION, AND/OR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES) IN CONNECTION WITH THE USE OF THIS MATERIAL.

IMDA RESERVES THE RIGHT TO CHANGE, MODIFY OR ADD TO ANY PART OF THIS DOCUMENT. NOTHING HEREIN IS INTENDED TO CREATE OR IMPOSE ANY BINDING LEGAL OBLIGATIONS OR LIABILITY WHATSOEVER ON IMDA, WHETHER EXPRESSED OR IMPLIED, AND WHETHER CONTRACTUAL OR OTHERWISE. WITHOUT PREJUDICE TO THE FOREGOING, NOTHING IN THIS DOCUMENT SHALL BIND IMDA TO ADOPT ANY PARTICULAR COURSE OF ACTION. CONSEQUENTLY, NOTHING HEREIN SHALL BE CONSTRUED AS GRANTING ANY EXPECTATION, WHETHER PROCEDURAL OR SUBSTANTIVE IN NATURE, THAT IMDA WILL TAKE OR NOT TAKE ANY PARTICULAR COURSE OF ACTION IN THE FUTURE, ARISING FROM OR DUE TO ANYTHING IN THIS DOCUMENT OR IN THE EXERCISE OF ITS DISCRETION AS A PUBLIC AUTHORITY.

IMDA DRAWS ATTENTION TO THE POSSIBILITY THAT ANY PRACTICE OR IMPLEMENTATION OF THIS STANDARD/SPECIFICATION MAY INVOLVE THE USE OF INTELLECTUAL PROPERTY RIGHTS AND TAKES NO POSITION CONCERNING THE EXISTENCE, VALIDITY AND/OR APPLICABILITY OF ANY SUCH INTELLECTUAL PROPERTY RIGHTS, WHETHER ASSERTED BY TSAC MEMBERS OR ANY THIRD PARTY.

AS OF THE DATE OF ISSUANCE OF THIS STANDARD/SPECIFICATION, IMDA HAS NOT RECEIVED WRITTEN NOTICE OF ANY PATENT RIGHTS WHICH MAY BE RELEVANT IN RELATION TO THE IMPLEMENTATION OF THIS STANDARD/SPECIFICATION. HOWEVER, IMPLEMENTERS ARE CAUTIONED THAT THIS MAY NOT REPRESENT THE LATEST INFORMATION AND ARE THEREFORE STRONGLY URGED TO CHECK WITH THE RELEVANT DATABASE IN ITU, ISO, IEC OR THE RELEVANT STANDARDS DEVELOPMENT ORGANISATION FOR INFORMATION OF INTELLECTUAL PROPERTY RIGHTS. IMPLEMENTERS ARE ADVISED TO OBTAIN THEIR OWN PROFESSIONAL, TECHNICAL AND/OR LEGAL ADVICE AND CONDUCT ALL NECESSARY DUE DILIGENCE, INCLUDING BUT NOT LIMITED TO MAKING SUCH INVESTIGATIONS OR SEEKING CLARIFICATIONS AS MAY BE APPROPRIATE, IN REGARD TO ANY DECISION OR ACTION THAT THEY INTEND TO TAKE, OR PRIOR TO THE IMPLEMENTATION OF ANY STANDARD/SPECIFICATION AS MAY BE REQUIRED.

1 Scope

The IMDA Reference Specification for Quantum Key Distribution Networks (RS QKDN) was published in June 2023 to guide the deployment and interoperability of QKDN infrastructure in Singapore. Building on this foundational specification, the Reference Specification for the Secure Deployment of QKDN focuses specifically on the security architecture, risks, and countermeasures needed to ensure the resilience and trustworthiness of QKDN implementations.

This security-focused specification provides practical guidance to safeguard the end-to-end operations of QKD networks (QKDNs). By aligning with this specification, implementers and operators can establish a robust security baseline that strengthens trust in QKD-enabled systems and ensures secure integration with conventional networks. This document references the ITU-T X.1710 security framework, which provides internationally recognised guidance on:

i. Security aspects for Quantum Key Distribution Networks (QKDNs);
ii. Security threats applicable to QKDNs across all architectural layers;
iii. Security requirements needed to address those threats; and
iv. Recommended security measures to mitigate risks and protect QKDN operations.

2 Abbreviations

This Reference Specification uses the following abbreviations:

API	Application Programming Interface
DoS	Denial of Service
EM	Electromagnetic
HMAC	Hash-based Message Authentication Code
IP	Internet Protocol
IPSec	Internet Protocol Security
ITU	International Telecommunication Union
IT-Secure	Information-Theoretically Secure
KM	Key Manager
KMA	Key Management Agent
MAC	Message Authentication Code
NM	Network Manager
NMS	Network Management System
PKI	Public Key Infrastructure
PSK	Pre-Shared Key
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QKDN	QKD Network
RS	Reference Specifications
SAE	Secure Application Entity
TLS	Transport Layer Security
TN	Trusted Node

3 Quantum Key Distribution Networks (QKDNs)

The conceptual architecture of a Quantum Key Distribution Network (QKDN) is specified in IMDA RS QKDN, which follows the ITU Y.3800 series. As shown in Figure 1 in IMDA RS QKDN, the QKDN architecture is organised into five logical layers: the quantum layer, the key management layer, the QKDN control layer, the QKDN management layer, and the service layer for applications. Entities in each logical layer are physically located within a QKD node. A QKD node is typically considered as a trusted node (TN), which resists any intrusions and attacks by unauthorised entities. A TN also acts as a boundary to secure the assets within the node from attackers outside the node.

In the quantum layer, pairs of QKD modules in different QKD nodes are connected by QKD links to generate identical random bit strings as QKD keys, based on the implemented QKD protocols. These QKD keys are pushed to the Key Manager (KM) within the same QKD node. The quantum layer also provides QKD module parameters, such as quantum bit error rate (QBER) and key generation rates, to the QKDN manager for network control and management.

The key management layer consists of KMs and KM links. It handles the processing, synchronisation, storage, and relay of received QKD keys. When a cryptographic application requests keys, the KM supplies the keys in the required format, ensuring they are synchronized between QKD nodes. This layer enables interoperability and scalability across the QKDN.

Control of QKD modules and KMs is handled by the QKDN control layer, which uses one or more controllers that may be centralised or distributed across QKD nodes. These controllers manage key relay routing, session authentication, link control, and quality-of-service policies. Meanwhile, the management layer oversees the overall health of the network, monitoring performance, security, configuration, and accounting functions.

The service layer enables secure applications by supplying them with keys generated by the QKDN. Through application interfaces, these keys allow users to establish secure communications using symmetric encryption between any two end nodes over the QKDN.

The design and deployment of a QKDN needs to consider security, scalability, robustness, efficiency, interoperability, and ease of integration to meet diverse users' and operational requirements. This document focuses on the security aspects of QKDN and follows the architecture and framework of QKDN that are defined in IMDA RS QKDN .

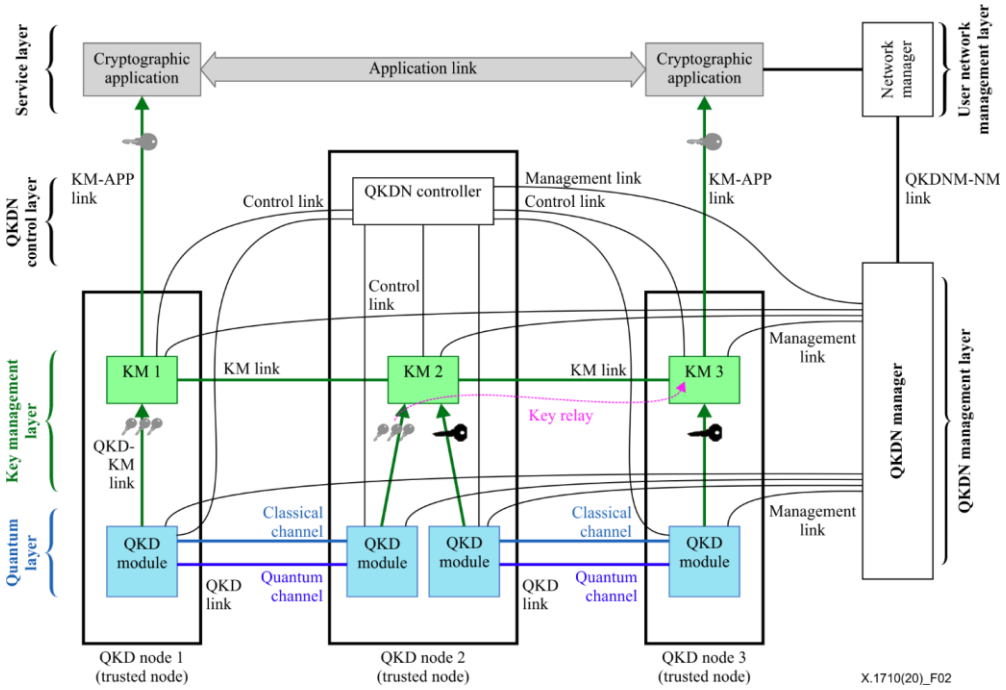

Figure 1: Typical structure of a QKDN and user network (Ref.: ITU-T X.1710 (10/2020))

3.1 Security Aspects specific to QKDN

The security of a QKDN is inherently multi-layered, corresponding to the five logical layers and addresses both quantum-specific threats and conventional cybersecurity risks. At the quantum layer, the core security assurance stems from the quantum mechanics principles, where any eavesdropping attempt on QKD links introduces detectable anomalies such as increased QBER. This enables QKD modules to discard compromised keys, ensuring the confidentiality of key generation. However, physical security of QKD devices and secure calibration processes remain essential to prevent tampering or side-channel attacks.

The key management layer guarantees the secure relay, synchronisation, and storage of QKD keys. Since keys may traverse multiple KMs before reaching the application, robust authentication and encryption mechanisms are critical to ensure trust across nodes, particularly in multi-domain or hybrid environments. Integrity checks and secure key lifecycle management are also crucial to prevent key leakage or misuse.

The QKDN control layer, responsible for orchestrating the operations of QKD modules and KMs, must be protected from control-plane attacks such as unauthorised access, spoofed commands, or routing manipulation. This layer relies on conventional IT security measures including role-based access control, cryptographic authentication and secure communication channels.

The management layer oversees network performance and security operations. It ensures secure logging, monitoring, configuration, and firmware management to defend against administrative compromise or insider threats. Secure boot and audit trails are recommended for forensic integrity.

Finally, the service layer interfaces with end-user applications thus enforcing strict access control and ensuring key isolation to prevent unauthorised use or exposure of cryptographic material is required. A secure QKDN requires the coordinated protection of all layers, blending quantum security principles with classical cybersecurity practices to deliver end-to-end confidentiality, integrity, and availability.

3.2 QKDN Security Threats

The security of a QKDN must address a wide range of threats that target both its quantum-specific components and classical infrastructure. It is essential to understanding these threats to ensure the confidentiality, integrity, and availability of the keys and services provided by the QKDN.

Quantum-Specific Threats:

i. Quantum Channel Eavesdropping: While QKD protocols can detect interception attempts through anomalies like increased QBER, attackers may still attempt to extract information by exploiting imperfections in photon sources or detectors.

ii. Quantum Hacking Attacks: These include detector blinding, Trojan-horse attacks, and timing attacks that exploit implementation weaknesses rather than the quantum protocol itself. Physical tampering or unintended emissions from QKD modules can also be used for side-channel exploitation.

iii. Denial of Service (DoS) on Quantum Channels: Malicious actors may disrupt the quantum link by injecting noise or blocking transmission, preventing successful key generation between QKD nodes.

Classical and Network-Level Threats:

i. Compromise of Key Management Systems (KMs): If KMs are accessed by unauthorised users or malicious insiders, keys may be leaked, altered, or improperly distributed. Weak authentication or insecure key relay links are primary risk vectors.

ii. Control Plane Attacks: The QKDN control layer is vulnerable to spoofed control messages, unauthorised configuration changes, and route manipulation attacks. These may lead to incorrect key routing or session hijacking.

iii. Management Plane Compromise: Improperly secured management interfaces or credentials can expose the QKDN to configuration tampering, firmware injection, or unauthorised monitoring.

iv. Application Interface Exploits: If access to the service layer is not well-controlled, applications or users could misuse or leak sensitive keys.

v. Supply Chain and Physical Security Risks: Tampered hardware or compromised firmware in QKD devices may introduce persistent vulnerabilities across the network.

Mitigating these threats requires a defence-in-depth approach that includes secure design, regular monitoring, and coordinated quantum and classical security controls across all QKDN layers.

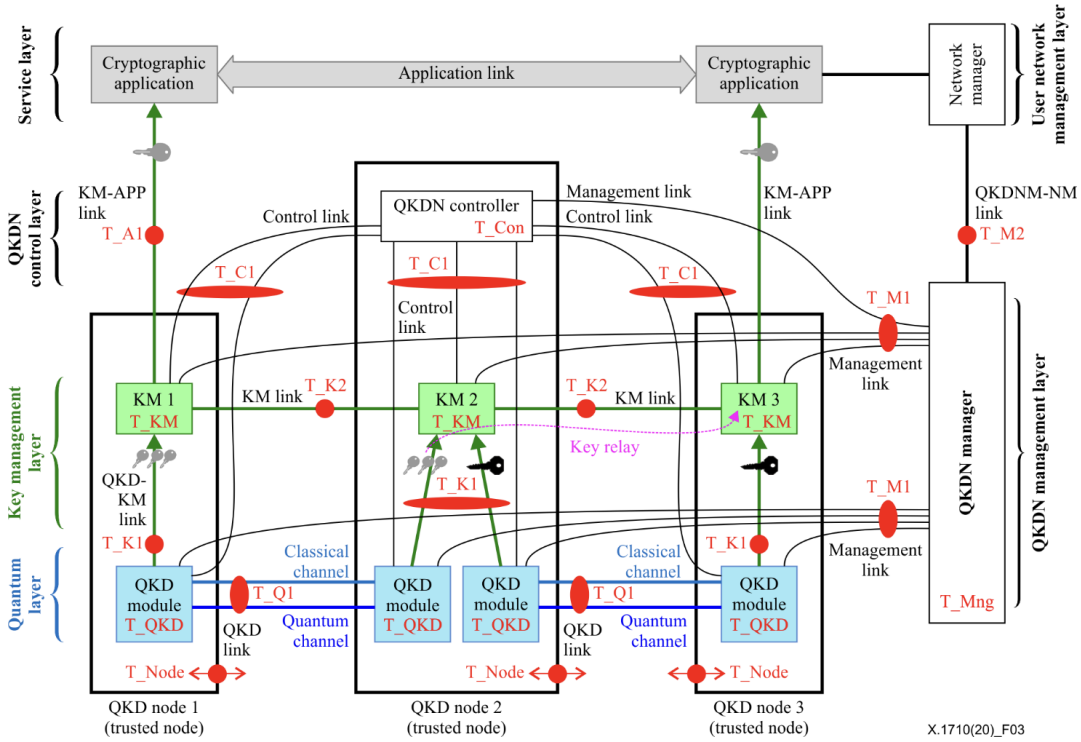

Figure 2: Security threats to QKDN (Ref.: ITU-T X.1710 (10/2020))

4 Security Aspects of Physical Trusted Node

4.1 Introduction to Trusted Node

QKD allows two distant parties to securely share symmetric random bit strings, which serve as cryptographic keys unknown to potential attackers. Any attempt to intercept these keys inherently disturbs the quantum states involved, making such eavesdropping detectable by the communicating parties. The information-theoretic security of QKD protocols is derived from the principles of quantum physics and quantum information theory, ensuring security independent of attackers' computational power. However, the range of point-to-point QKD links is fundamentally constrained by quantum channel losses as mentioned in ITU-T FG QIT4N 2.3.1. To overcome this limitation and enable long-distance key distribution, QKDNs can employ approaches such as quantum repeaters and TNs to extend their communication ranges. TN based QKDNs are mature enough to implement widely in practice, while they also support a variety of QKD-based applications. In this RS, if not mentioned specifically, all the security aspects are related to TN based QKDNs.

The trustworthiness aspect and the security aspect of the QKD node are fundamental elements to ensure the overall security in QKDN. It has been shown that a partially corrupted QKD node can lead to failures of the security of keys when keys are relayed using the corrupted QKD node where no honest path exists, and potentially in other insecure circumstances as mentioned in ITU-T X.1713. At a basic level, the security of a QKDN can be analysed under the assumption that QKD nodes have been configured to be secure and that they keep QKDN physical entities out of reach of attackers aside from links between QKD nodes. In practice, such assumptions give rise to a few security requirements. This section mainly refers to ITU-T X.1713.

4.2 Security Threats

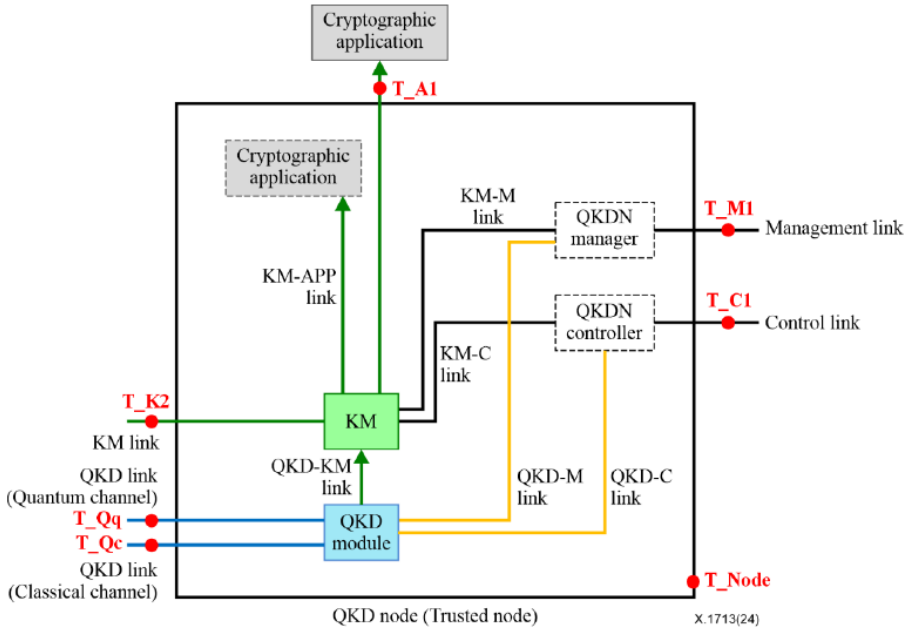

Figure 3: A typical structure of a QKD node and security threats (Ref.: ITU-T X.1713 (04/2024))

4.2.1 Within TN (boundary access)

i. Unauthorised physical access

A QKD node can be compromised physically through various means, such as exploiting weaknesses in access control systems, misconfigurations like weak passwords, or by impersonating authorised personnel. Once inside, attackers can target components such as QKD modules, key managers (KMs), and their interfaces (e.g., QKD-KM, KM-APP, KM-C, KM-M, QKD-C, QKD-M), as well as the QKDN controller, manager and other entities inside the QKD node. Their objectives typically include stealing sensitive information or conducting malicious activities like data tampering, impersonation, DoS, forgery, or repudiation. Additionally, attackers can disrupt, manipulate, or even take control of the physical entities and interfaces within the QKDN.

ii. Unauthorised access through dynamic entities

To support cryptographic applications outside the TN, certain entities can be entering and leaving a QKD node. For instance, cryptographic applications may involve mobile devices like smartphones or drones, which receive keys within the QKD node but typically use them outside it. In such scenarios, attackers can introduce unauthorised mobile devices into the QKD node to interact with internal components for malicious purposes.

iii. Attacks through installation, maintenance and migration

Attackers can target QKD node components during installation, maintenance, or migration by introducing backdoors or inserting unauthorised modules such as QKD modules, key managers, or QKDN controllers and managers. Additionally, certain QKD modules include maintenance ports used to verify device functionality. If these ports are not properly secured or disabled, they can be potential entry points for attacks.

iv. Classical side-channel attacks

Classical side-channel attacks pose threat to cryptographic modules inside a QKD node. These attacks typically involve monitoring outputs from the modules such as power consumption, radiative electromagnetic (EM) signals, etc. or applying external factors like EM waves, or manipulating temperature and voltage. Both invasive and non-invasive methods can pose threats to a QKD node.

4.2.2 Across TNs (Interfaces to the TN)

i. Unauthorised network access

Attackers may attempt to gain access to the functional components inside the QKD node via external links and interfaces, which can pose threats (T_Qc, T_K2, T_C1, T_M1, T_A1) such as unauthorised access to information assets, exploitation of cryptographic weaknesses, abuse of system functions, cascading failures, evasion of audit mechanisms, and deployment of malicious updates.

ii. Attacks against the QKD link

In a QKD node, the quantum channel is an open channel for the QKD transmitter and receiver to exchange quantum signals, attackers can send light into QKD modules to affect the behaviours of internal components or to detect light leakage via the quantum channel (T_Qq), which can enable attackers to achieve knowledge of key information without being detected [ITU-T FG-QIT4N TR D2.3]. Insertion or leakage of light is always possible, even if the QKD node and QKD modules have their own security enclosure. For the classical channel the post-processing information can be modified by the attacker if there are vulnerabilities on the integrity protection, which can also lead to leakage of key information (T_Qc).

To help promote better understanding, an example of a threat modelling analysis of the QKDN TN, grounded in the MITRE ATT&CK® framework is described in Annex A for illustration purpose.

4.3 Security Recommendations and Measures

4.3.1 Within TN (boundary access)

i. Confidentiality

Shielding the entire installation site is beneficial both to prevent EM emissions from escaping the equipment and to block external EM radiation attacks.

Recommendations

Based on the layout of the station and the system architecture, the required level of EM wave attenuation for the QKD node can be determined, with the shielding design tailored to the specific environmental conditions.

ii. Access Control

Setting up boundary protection in a QKD node helps to secure against physical intrusion by adversary entities into areas containing its QKDN physical entities and links between them. Additionally, having physical protection provides extra security to its QKDN physical entities and the links between them. The QKD node has the capability to trace the physical access in a QKD node help to provide surveillance on the QKD nodes.

Recommendations

Implementing door access control, intrusion detection, and/or alarms for the QKD node provides an effective boundary protection. For example, physical access implemented by multi-factor authentication using an integrated circuit card, biometric authentication or passcode/password authentication using a numerical keypad provide physical access control. Identification for physical access by personnel such as security guards, anti-pass packs, interlock controls further prevent unauthorised physical access. Additional physical protection such as secure cages, and tamper protection mechanisms provide additional layers of security. Furthermore, installation of local/remote video monitoring system can prevent unauthorised physical access.

iii. Availability

The QKD node monitors environmental parameters and reports significant deviation from typical operations. Physical protection measures in a QKD node protects against accidental physical damage due to environmental factors, such as fires, to its QKDN physical entities and the links between them.

Recommendations

The QKD node uses real-time sensors to monitor the surrounding parameters, such as temperature, power supply voltage and humidity level.

Installation of a fire detection system provides detection of fire early and minimises the impact, for example through the incorporation of ultra-sensitive very early smoke detection apparatus (VESDA) smoke detection system in the air circulation system. A gas-based fire extinguishing system causes less damage to equipment, hence is a preferred option.

4.3.2 Across TNs (QKD link and Classical link interface on the QKD node)

i. Confidentiality

To protect against attacks on the quantum channel, QKD node can optionally aid the QKD modules to reduce possible light injections from an attacker to the QKD modules via the quantum channel, and to prevent unwanted light leakage of QKD modules to the quantum channel.

Recommendations

In the QKD node, addition of active or passive components such as light monitors, isolators, circulators, filters or power meters to the quantum channel in the QKD links to reduce light injection to or light leakage from the quantum channel.

NOTE: Active or passive components can be added to the QKD node on the interface of quantum channel in the QKD link. Such measures may interfere with the correct operation of QKD modules, which may need further customisation on QKD modules.

ii. Integrity

Implementation of measures against threats T_Qc, T_A1, T_K2, T_M1 and T_C1 in a QKD node protects the integrity of information in the relevant links by ensuring the correctness of stored and transferred data, protecting against modification, deletion, creation (insertion) and replay of exchanged data.

Recommendations

A QKD node uses cryptographic algorithms with appropriate computational security, including post-quantum cryptographic techniques and IT-secured methods (e.g. Wegman-Carter message authentication code) to protect the integrity of the data transfer.

5 Security Aspects of Quantum Layer

5.1 Introduction to Quantum Layer

This clause describes the security aspects of entities in the quantum layers in the QKDN, which include QKD modules located in a QKD node ; QKD links, i.e. quantum channels and classical channels and QKD key interfaces to the key manager located in the same QKD node from a QKDN perspective. The main focus is on the security requirements and measures for QKD modules and their channels to be secure against quantum side channel attacks. It also introduces the security aspects of the quantum layer with confidentiality, integrity, and availability analysis. For illustration purposes, it also covers some examples of implementation security of QKD modules as well as general descriptions of QKD protocols.

This clause mainly refers to ITU-T X.1710, X.1713 and ITU-T FG QIT4N D2.3.

5.2 Security Threats

5.2.1 Within TN

i. T_QKD: Security threats at the QKD module through the QKD link, control link or management link:
   - deletion or corruption: deleting or modifying the information in the QKD module;
   - DoS: denial of access or flooding data traffic

ii. T_K1: Security threat at the QKD-KM links:
   - eavesdropping: intercepting and deciphering the key data and the metadata;
   - deletion or corruption: deleting or modifying the key data and the metadata;
   - DoS: communication interruption or flooding data traffic

5.2.2 Across TNs (QKD Modules and QKD links)

i. T_Qq and T_Qc: Security threats at the QKD link:
   - eavesdropping (T_Qq): An eavesdropper can gain secret key information of the QKD modules through quantum side-channel attacks via the quantum channel;
   - deletion or corruption (T_Qc): deleting or modifying the information in the classical channel;
   - DoS (T_Qq, T_Qc): communication interruption or flooding data traffic.

ii. Implementation attacks on QKD modules

In the quantum layer, the major security threats are due to the quantum side-channel attacks (T_QKD, T_Qq), which is also known as implementation attacks, or quantum hacking attacks on QKD modules ITU FG QIT4N TR D2.3.

The security of QKD protocols implemented on QKD modules depends on certain assumptions. In practice, real-world QKD module implementations sometimes deviate from the idealised models used in security proofs of QKD protocols. Such deviations may introduce vulnerabilities that allow an eavesdropper to exploit attacks and compromise the security of practical QKD systems. When combined with specific attack strategies, various types of side-channel attacks targeting QKD modules have been demonstrated to be feasible. Some of these attacks have already been realised using current technologies, posing immediate threats to QKD networks by enabling an eavesdropper to gain partial or even full access to the secret keys.

Threats to QKD modules (T_QKD) primarily arise at the QKD link ports, which serve as the interface between the QKD transmitter and receiver between two TNs. Through these ports, an eavesdropper may inject light to interfere with internal components, detect leaked light that may contain key information, or send probe light and analyse its reflections to infer key encoding details (T_Qq). Since the quantum channel is an open channel for exchanging quantum signals, even if the internal components are protected within its own secure packaging, an eavesdropper can still transmit or receive optical signals via the link ports. Meanwhile, the eavesdropper is also allowed to listen and copy all the information that is exchanged via the classical channel (T_Qc).

On the other hand, while attacks targeting QKD modules are theoretically feasible, they are generally way more challenging to execute in real-world environments compared to attacks conducted remotely via pure digital means. Such attacks also require optical layer access with optical quantum signals to interact with QKD module's operations. Consequently, an eavesdropper would need to physically tap into the QKD link and establish a station between the two QKD nodes to carry out their attack strategy. Moreover, some of the attacks on QKD implementations are only possible in theory and require future advancement in technology; some of the attacks are proven to be feasible by violating the assumptions in security proof, but without a specific strategy. The threat assessment of the implementation attacks on QKD is out of scope of this document.

5.3 Security Recommendations and Measures

5.3.1 Within TN

i. Confidentiality

The key data and the metadata are encrypted and protected when the key is transferred from the QKD module to the KM via the QKD-KM link.

Recommendations

Implementation of appropriate end-to-end encryption protocols maintains the confidentiality of the key transfer. Physical protection of the link can be included as well.

ii. Integrity

Implementation of measures against threats T_K1 protects the integrity of information in the relevant links by ensuring the correctness of stored and transferred data, protecting against modification, deletion, creation (insertion) and replay of exchanged data.

Recommendations

The QKD Module to KM link uses cryptographic algorithms with appropriate computational security, including post-quantum cryptographic techniques and IT-secured methods (e.g. Wegman-Carter message authentication code) to protect the integrity of the data transfer.

iii. Access Control

The TN ensures that only authorised entities have access to the resources concerned, including physical systems, system software, applications or data.

Recommendations

The access control information specifies a means to determine which entities are authorised to have access, and the kind of access allowed. Authentication functions further support the access control.

iv. Availability

Fallback option for hardware failure ensures the QKD module remains operational. Network resilience for the QKD Module to KM ensures the availability of the key data to continue providing acceptable level of service.

Recommendations

Additional hardware components such as redundant power supply prevents interruptions due to power supply failure. Appropriate security measures on network resilience support adaptations and recovery from disruptions and security threats. In the event of security violation, damage can be minimised in a controlled manner. A system recovery mechanism will ensure the system to be restored to the required security level.

v. Accountability

Capturing the records of security critical action and the key metadata ensures that the functional elements involved can be uniquely traceable.

Recommendations

Activity logging supports the storing of the security information and the key metadata (including the QKD module(s) involved). Security audit allows the logged data to be analysed on security events.

5.3.2 Across TNs (QKD Modules and QKD links)

i. Confidentiality

Protection against Quantum side-channel attacks mitigates the attacks from an eavesdropper exploiting potential implementation loopholes of QKD modules via the quantum channel.

Recommendations

By including appropriate countermeasures against quantum side-channel attacks in the QKD modules including both QKD transmitter and QKD receiver, the impact of the attacks on the QKD modules can be minimised. The main objective of the countermeasures is to ensure that there is no unwanted light leakage and injection into QKD transmitter and/or QKD receiver, and to ensure the correct operation status of the components in QKD modules. Some examples of the techniques include active or passive components such as light monitor, isolator, circulator, filter or power meter. The validation of these countermeasures methods is outside the scope of this document.

ii. Integrity

Implementation of measures against threats T_Qc protects the integrity of information in the relevant links by ensuring the correctness of stored and transferred data, protecting against modification, deletion, creation (insertion) and replay of exchanged data.

Recommendations

The classical channel of the QKD link uses cryptographic algorithms with appropriate computational security, including post-quantum cryptographic techniques and IT-secured methods (e.g. Wegman-Carter message authentication code) to protect the integrity of the data transfer.

iii. Availability

Implementation of counter-measures against DoS attacks (T_Qq, T_Qc) ensures the availability of the QKD links.

Recommendations

Switching to backup quantum channel link using optical switch due to optical link reduction or cutoff; switching to back up classical channel link due to DoS attacks on the classical channel.

iv. Accountability

Capturing the records of security relevant activities of the QKD links ensures that the information of the events caused by T_Qq and T_Qc can be traceable.

Recommendations

Activity logging supports the storing of the security information. Security audit allows the logged data to be analysed on security events.

6 Security Aspects of Key Management Layer

6.1 Introduction to Key Management Layer

The key management layer, as defined in ITU-T X.1712, is a critical component within the overall cybersecurity and secure communications framework for QKDN as it is responsible for the generation, distribution, storage, use, and lifecycle management of cryptographic keys. The key management layer serves as a foundational security service that supports confidentiality, integrity, authentication, and non-repudiation by enabling secure cryptographic operations across diverse systems and environments. It also ensures that cryptographic keys are handled in a secure, standardised, and interoperable manner, minimising risks associated with unauthorised access, key leakage, or misuse.

This layer operates across several functional areas including policy enforcement, key generation and registration, secure key distribution mechanisms, and key lifecycle controls such as activation, expiration, revocation, and destruction. It interfaces with multiple entities including end-user systems, security modules, trusted authorities, and applications, enforcing strong cryptographic policies and audit mechanisms to maintain trust and compliance. ITU-T X.1712 highlights the need for scalable and interoperable key management architectures that support hierarchical, distributed, and hybrid trust models, especially in multi-domain or federated environments. By establishing a structured approach to key management, this layer supports secure digital communications, facilitates lawful access under controlled circumstances, and enables robust cybersecurity strategies in both public and private sector systems.

6.2 Security Threats

The key management layer becomes a high-value target for a wide range of security threats due to its central role in enabling end-to-end quantum-safe communication. These threats can arise from internal compromises within TNs, vulnerabilities in inter-node communication links, or weaknesses in interfaces with application entities such as the Secure Application Entity (SAE).

6.2.1 Within TN

i. **Insider Threats**: Malicious or careless insiders may access or misuse cryptographic keys and sensitive key management functions.

ii. **Compromise of Key Management Agent (KMA**): If the KMA is compromised, it could lead to unauthorised key generation, distribution, or revocation.

iii. **Malware and Software Vulnerabilities**: Exploiting flaws in the software stack can allow attackers to gain unauthorised access to stored keys or manipulate key lifecycle events.

iv. **Improper Access Control:** Weak or misconfigured access controls may allow unauthorised entities to interact with or extract keys.

6.2.2 Across TNs

i. **Man-in-the-Middle (MitM) Attacks**: Intercepting and potentially altering key material or control messages between nodes.

ii. **Eavesdropping**: Unauthorised listening to unencrypted or poorly protected communication can lead to key leakage.

iii. **Replay Attacks**: Capturing and reusing valid key distribution messages to trick nodes into accepting compromised keys.

iv. **Message Tampering**: Alteration of messages in transit to disrupt synchronisation or inject malicious keys.

6.2.3 KM to SAE

i. **Interface Hijacking**: Unauthorised entities could hijack or mimic the SAE interface to request or access keys illegitimately.
ii. **Improper Binding or Weak Authentication**: Weak authentication mechanisms between KMA and SAE could allow impersonation or unauthorised access to keys.

iii. **Data Leakage through Improper** Application Programming Interface **(API) Usage**: Unsecured APIs or poorly designed integration could result in accidental exposure of sensitive keying material.

iv. **Denial-of-Service (DoS):** Overwhelming the interface could prevent legitimate applications from obtaining cryptographic services.

6.3 Security Recommendations and Measures

The key management layer requires robust security measures to defend against threats from internal node compromises, insecure links, and weak interfaces with application entities like the SAE. To ensure trust and resilience, security recommendations and measures have to address confidentiality, integrity, availability, and authentication through layered controls such as encryption, secure hardware, strong authentication, and continuous monitoring.

6.3.1 Within TN

i. Confidentiality

To maintain a secure environment, it is essential that cryptographic keys and sensitive operational data within a TN are kept confidential at all times. Unauthorised access to these keys could compromise the entire network.

Recommendations

Maintaining confidentiality involves the use of tamper-resistant hardware such as Hardware Security Modules to isolate and safeguard cryptographic keys and sensitive operations. Enforcing strict access control policies that limit key access to trusted components and authorised personnel is a foundational measure. Additionally, applying secure memory management techniques and encrypting both transient and persistent data helps to ensure protection throughout the key's lifecycle.

ii. Availability

Reliable and continuous operation of key management functions within a TN is essential to maintain overall system availability and prevent service disruption.

Recommendations

Ensuring availability can be achieved by deploying redundant KMA instances with automatic failover capabilities. Load balancing across nodes supports consistent performance under high load conditions. Proactive monitoring mechanisms help detect system anomalies early, enabling timely intervention. It is also beneficial to design key management systems with graceful degradation features, allowing critical services to remain functional even when auxiliary components encounter issues.

iii. Authentication

Verifying the identity of system entities and administrators within the TN is important to prevent unauthorised access control or misuse.

Recommendations

Effective identity verification can be implemented by adopting multi-factor authentication methods for all administrative activities. Establishing role-based access controls helps align system privileges with specific responsibilities, minimising risk exposure. Logging and auditing all access events further enhance accountability and allow for retrospective analysis in the case of security incidents. For system entities such as KMAs and application interfaces, mutual authentication using digital certificates or cryptographic tokens is essential to prevent impersonation and unauthorised access.

iv. Integrity

Safeguarding the integrity of key material and system components ensures that they remain accurate, untampered, and trustworthy during operation.

Recommendations

Cryptographic hashing and digital signature mechanisms offer assurance that configurations, binaries, and stored data have not been altered. Secure boot processes provide integrity checks during system initialisation, preventing tampered software from executing. Periodic integrity verification routines within the operating environment can further detect and isolate unexpected modifications promptly.

6.3.2 Across TNs

i. Confidentiality

Protecting the confidentiality of key data exchanged between TNs is fundamental to prevent eavesdropping and information leakage.

Recommendations

Establishing encrypted communication channels using secure protocols such as Transport Layer Security (TLS) 1.3 or Internet Protocol Security (IPSec) ensures the confidentiality of data in transit. In cases where higher levels of secrecy are necessary, techniques like one-time pad encryption may be employed. Encrypting key materials individually before transmission offers an added layer of protection, especially when traversing shared or untrusted infrastructure.

ii. Availability

The KMAs are required to maintain the availability of secure KMA links for key relay and management operations.

Recommendations

Building communication paths with redundancy and incorporating automatic failover mechanisms help mitigate the effects of physical or logical link failures. Defensive techniques such as DoS mitigation tools and rate limiting further bolster link reliability. Additionally, supporting queuing, retry logic, and intelligent timeout configurations allow the system to handle intermittent network disruptions gracefully.

iii. Authentication

Ensuring that only legitimate TNs can engage in key exchanges reduces the risk of impersonation and malicious activity.

Recommendations

Mutual authentication using IT-secure authentication or digital certificates supported by a public key infrastructure strengthens trust in inter-node communication. Regular validation of certificate status, including expiration and revocation, helps ensure that outdated or compromised credentials are not accepted. When appropriate, incorporating device-level attestation adds another layer of assurance by confirming the integrity of the communicating hardware.

iv. Integrity

The correctness and consistency of key exchange messages between nodes must be verifiable to prevent alteration or replay.

Recommendations

Attaching cryptographic integrity checks, such as message authentication codes (MACs) or digital signatures, to all exchanged messages helps detect unauthorised changes. Incorporating anti-replay mechanisms—such as sequence numbers, timestamps, and nonces—can identify and discard duplicated or stale messages. Logging integrity failures support early detection of network-based attacks or system misconfigurations.

6.3.3 KM to SAE

i. Confidentiality

The confidentiality of key material shared between the KMA and the SAE must be maintained to prevent interception or misuse.

Recommendations

To protect confidentiality, IT-secure encrypted communications should be enforced between the KMA and SAE, using end-to-end encryption protocols such as mutual TLS. Even within secure channels, encrypting the key payload itself provides an additional safeguard. Regular rotation of session keys minimizes the impact of any single compromised session and enhances ongoing confidentiality protection.

ii. Availability

The interface between the KMA and SAE must remain accessible and responsive to support application-level cryptographic operations.

Recommendations

Designing the interface to be scalable allows it to handle demand surges and system growth effectively. Implementing rate limiting ensures fair use while preventing abuse. To further enhance reliability, caching frequently accessed keys and incorporating automatic retries can help reduce operational delays caused by transient faults. Continuous monitoring facilitates rapid response to potential outages or performance degradation.

iii. Authentication

Access to key management functions and key material by the SAE must be restricted to verified and authorised components.

Recommendations

Strong authentication of SAEs can be achieved through the use of digital certificates, signed tokens, or similarly robust mechanisms. Policy-based access controls help evaluate whether a given request aligns with defined trust and usage rules. Binding delivered key material to a specific SAE or session ensures that even if the material is intercepted, it cannot be misused by unauthorised entities.

iv. Integrity

Key material and control messages exchanged with the SAE must remain unaltered from their origin to their destination.

Recommendations

Using digital signatures or Hash-based Message Authentication Codes (HMACs) on all messages helps detect and prevent unauthorised modifications. Input validation measures ensure that transmitted data conforms to expected formats, reducing the risk of injection attacks or unintentional corruption. Any message that fails integrity checks shall be rejected and logged for further investigation, helping maintain system trustworthiness.

7 Security Aspects of Control & Management Layer

7.1 Introduction to Control & Management Layer

The QKDN controllers exercise controls towards key management and quantum layers to provide functions including key relay routing, session control of services provided by QKD, authentication and authorisation, QoS and charging policies for a QKDN. Depending on the implementation, the controller function may be centralised in one node or distributed across multiple nodes.

The QKDN management layer provides functional configuration to the different QKDN modules, QKDN controller, Key management, QKD module and Network manager. It covers the QKDN manager and associated software elements, the fault management, the configuration management, the account management, the performance management and the security management. The QKDN manager is in a different physical location than the QKD node.

The information provided in this section is based on the Recommendation ITU-T X.1710, X.1712, X.1713, X.1716, X.1717.

7.2 Security Threats

The control and management layer is a high-value target for security threats due to its central role in orchestrating QKDN operations and managing critical information assets. These threats can arise from vulnerabilities in communication links within and across TNs, between controllers and managers, and within the QKDN manager itself.

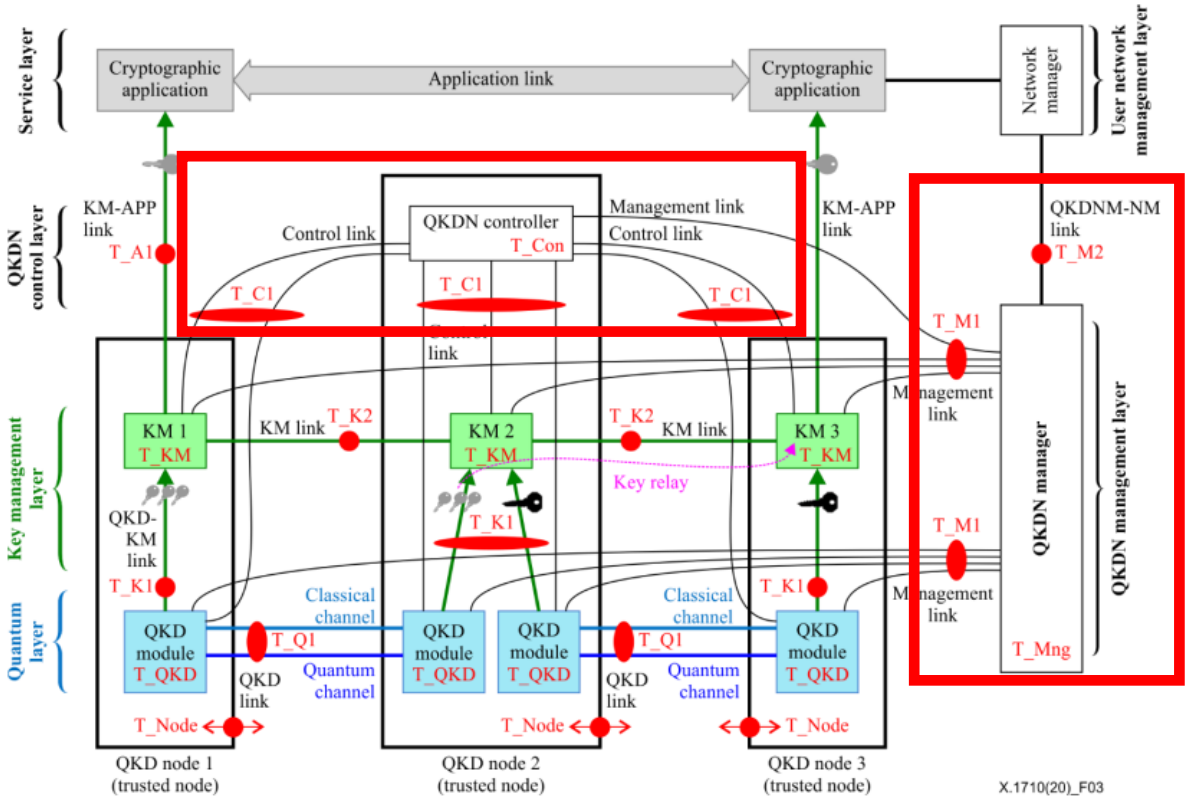

Figure 4: Security threats to the Control & Management Layer of QKDN (Ref.: ITU-T X.1710 (10/2020))

7.2.1 Within TN

i. Communication link between QKDN controller and the KM functional element is an attack surface where information assets like key routing table, key pool status, service health, session information, QKDN topology, access and authorisation can be compromised via security threats like eavesdropping, deletion, corruption or interruption by DoS.

ii. Communication link between QKDN controller and the QKD element is an attack surface where information assets like QKD link control information, QBER status, QKD status and failure diagnosis and access and authorisation can be compromised via security threats like deletion, corruption or interruption by DoS.

7.2.2 Across TNs

i. In the case of a centralised controller architecture, the communication links between QKDN controller and KM and QKD functional elements are attack surfaces for security threats like eavesdropping, deletion, corruption or interruption by DoS.

ii. In the case of a distributed controller architecture, the communication links between QKDN controllers are attack surfaces for security threats like eavesdropping, deletion, corruption or interruption by DoS.

7.2.3 Controller to QKDN Manager

i. Communication link between the QKDN controller and QKDN manager is an attack surface where fault, configuration, accounting, performance and security management information may transit between the controller and manager can be compromised via security threats like eavesdropping, deletion, corruption or interruption by DoS.

7.2.4 QKDN Manager to TNs

i. Communication link between the QKDN manager and the KM functional element is an attack surface where information assets like KM configuration can be compromised via security threats like eavesdropping, deletion, corruption or interruption by DoS.

7.2.5 QKDN Manager to Network Manager (NM)

i. Communication link between the QKDN manager and the Network manager functional element is an attack surface where monitoring information from the QKDN to the user Network Manager System (NMS)can be compromised via security threats like eavesdropping, deletion, corruption or interruption by DoS.

7.2.6 Within QKDN manager

i. The configuration inside the QKDN manager may be at risk of spoofing, repudiation or interruption by DoS.

7.3 Security Recommendations and Measures

The control and management layer requires robust security measures to protect against threats to communication links and internal processes. These measures address confidentiality, integrity, authentication, and availability through layered controls such as encryption, physical protection, strong authentication, and resilience mechanisms.

7.3.1 Within TN

i. Confidentiality

The confidentiality of control information assets transiting within communication links between the QKDN controller and the KM and QKD functional elements must be maintained to prevent unauthorised access or leakage.

Recommendations

The QKDN controller should ensure that control information assets are protected by appropriate physical protection measures, such as tamper-resistant hardware, and/or cryptographic means, such as encryption protocols implemented through a Public Key Infrastructure (PKI). Physical protection within TNs may include tamper protection mechanisms to safeguard sensitive data and operations.

ii. Integrity

The integrity of control information received from KM and QKD functional elements must be ensured to maintain accuracy and trustworthiness.

Recommendations

The QKDN controller should authenticate the identity of KM and QKD functional elements and verify their authorisation levels to ensure the integrity of control information received. Cryptographic mechanisms, such as tamper-resistant hardware, message authentication codes (MACs) or digital signatures, should be used to detect unauthorised modifications. Regular integrity checks should be performed to identify and isolate any tampering or corruption.

iii. Authentication

Verifying the identity of entities within the TN is critical to prevent unauthorised access or misuse of control functions.

Recommendations

The QKDN controller should perform mutual authentication with KM and QKD functional elements using cryptographic protocols, such as using IT-secure authentication (e.g. Wegman-Carter message authentication code), TLS with PKI, Pre-Shared Key (PSK), or hybrid-based algorithms. Explicit authentication schemes, such as those using digital certificates or cryptographic tokens, should be adopted to ensure that only authorised entities can access control information. Role-based access controls should be implemented to align privileges with responsibilities.

iv. Availability

The reliable and continuous operation of control functions within a TN is essential to prevent service disruptions.

Recommendations

The QKDN controller should support protection and recovery mechanisms, such as redundant controller instances with automatic failover capabilities, to enhance resiliency and robustness. Load balancing and proactive monitoring should be implemented to maintain consistent performance and detect anomalies early. Designing systems with graceful degradation features ensure that critical control functions remain operational during partial system failures.

7.3.2 Across TNs

i. Confidentiality

The confidentiality of control information assets transiting between QKDN controllers or between controllers and KM and QKD functional elements must be protected to prevent eavesdropping or leakage.

Recommendations

In both centralized and distributed controller architectures, the QKDN controller should ensure that control information is protected by cryptographic means, such as TLS or IPsec, implemented through a PKI infrastructure. Encrypting sensitive data before transmission across shared or untrusted infrastructure provides an additional layer of protection.

ii. Integrity

The integrity of control information exchanged between controllers or with KM and QKD functional elements must be verifiable to prevent alteration or corruption.

Recommendations

The QKDN controller should use cryptographic integrity checks, such as MACs or digital signatures, to detect unauthorised changes to messages that are exchanged. Anti-replay mechanisms, including sequence numbers, timestamps, or nonces, should be incorporated to identify and discard duplicated or stale messages. Logging integrity failures supports early detection of network-based attacks or misconfigurations.

iii. Authentication

Ensuring that only legitimate controllers and functional elements can engage in control information exchanges reduces the risk of impersonation.

Recommendations

Mutual authentication using IT-secure authentication or digital certificates supported by a PKI should be implemented to strengthen trust in inter-controller or controller-to-functional-element communications. Regular validation of certificate status, including expiration and revocation checks, ensures that compromised credentials are not accepted. Device-level attestation may be used to confirm the integrity of communicating hardware.

iv. Availability

The availability of communication links between controllers or with KM and QKD functional elements must be maintained to support control operations.

Recommendations

Communication paths should be built with redundancy and automatic failover mechanisms to mitigate the effects of link failures. DoS mitigation tools and rate limiting should be employed to enhance link reliability. Queuing, retry logic, and intelligent timeout configurations should be supported to handle intermittent network disruptions gracefully.

7.3.3 Controller to QKDN Manager

i. Confidentiality

The confidentiality of management information transiting between the QKDN controller and QKDN manager must be maintained to prevent interception or misuse.

Recommendations

Encrypted communication channels, such as mutual TLS, should be enforced between the QKDN controller and QKDN manager to protect management information. Encrypting the management payload itself provides an additional safeguard. Regular rotation of session keys minimises the impact of compromised sessions and enhances confidentiality.

ii. Integrity

Management information exchanged between the QKDN controller and QKDN manager must remain unaltered to ensure trustworthiness.

Recommendations

Digital signatures or HMACs should be used on all messages to detect unauthorised modifications. Input validation measures should ensure that transmitted data conforms to expected formats, reducing the risk of injection attacks or corruption. Messages failing integrity checks should be rejected and logged for further investigation.

iii. Authentication

Access to management functions and information by the QKDN manager must be restricted to verified and authorised entities.

Recommendations

Strong authentication of the QKDN manager should be achieved through IT-secure authentication, digital certificates, signed tokens, or similar mechanisms. Policy-based access controls should evaluate whether requests align with defined trust and usage rules. Binding management information to specific sessions ensures that intercepted data cannot be misused by unauthorised entities.

iv. Availability

The interface between the QKDN controller and QKDN manager must remain accessible and responsive to support management operations.

Recommendations

The interface should be designed to be scalable to handle demand surges and system growth. Rate limiting should be implemented to prevent abuse, and caching frequently accessed management data can reduce delays caused by transient faults. Continuous monitoring should facilitate rapid response to potential outages or performance degradation.

7.3.4 QKDN Manager to TNs

i. Confidentiality

The confidentiality of management information transiting between the QKDN manager and KM functional elements must be protected to prevent unauthorised access.

Recommendations

The QKDN manager should protect management links with physical protection measures and/or cryptographic methods, such as TLS or IPsec. Encrypting KM configuration data before transmission provides an additional layer of security, especially across untrusted infrastructure.

ii. Integrity

The integrity of management information, such as KM configuration, must be ensured to prevent tampering or corruption.

Recommendations

The QKDN manager should verify the integrity of management information received from KM functional elements using cryptographic mechanisms like digital signatures or HMACs. Regular integrity checks should detect unauthorised modifications, and any failures should be logged for investigation.

iii. Authentication

Access to management functions by KM functional elements must be restricted to verified and authorised entities.

Recommendations

Mutual authentication between the QKDN manager and KM functional elements should be performed using cryptographic protocols like IT-secure authentication, TLS with PKI or PSK. Policy-based access controls should ensure that only authorised elements can access or modify management information. Explicit authentication schemes should be adopted to prevent impersonation.

iv. Availability

The communication link between the QKDN manager and KM functional elements must remain available to support management operations.

Recommendations

Redundant communication paths and automatic failover mechanisms should be implemented to mitigate link failures. DoS mitigation tools and rate limiting should enhance link reliability. Queuing and retry logic should handle intermittent disruptions, and continuous monitoring should detect performance issues early.

7.3.5 QKDN Manager to NM

i. Confidentiality

The confidentiality of monitoring information transiting between the QKDN manager and the network manager (NM) must be maintained to prevent unauthorised access.

Recommendations

Encrypted communication channels, such as mutual TLS, should be enforced between the QKDN manager and NM. Encrypting monitoring data before transmission provides an additional safeguard, particularly across shared infrastructure.

ii. Integrity

Monitoring information exchanged with the NMS must remain unaltered to ensure accuracy and trustworthiness.

Recommendations

Digital signatures or HMACs should be used to detect unauthorised modifications to monitoring data. Input validation should ensure data conforms to expected formats, and messages failing integrity checks should be rejected and logged for investigation.

iii. Authentication

Access to monitoring information by the NM must be restricted to verified and authorised entities.

Recommendations

Strong authentication of the NM should be achieved through digital certificates or signed tokens. Policy-based access controls should verify that requests align with defined trust rules. Binding monitoring data to specific sessions prevents misuse by unauthorised entities.

iv. Availability

The communication link between the QKDN manager and NMS must remain accessible to support monitoring operations.

Recommendations

The interface should be scalable to handle increased demand, with rate limiting to prevent abuse. Caching frequently accessed monitoring data and incorporating retry logic can reduce delays. Continuous monitoring should enable rapid response to outages or performance degradation.

7.3.6 Within QKDN Manager

i. Confidentiality

The confidentiality of configuration data processed within the QKDN manager must be protected to prevent unauthorised access or leakage.

Recommendations

The QKDN manager should employ tamper protection measures, such as tamper-resistant hardware, and/or cryptographic measures to safeguard configuration data. Encrypting sensitive data at rest and in transit within the manager enhances confidentiality protection.

ii. Integrity

The integrity of configuration data processed within the QKDN manager must be ensured to prevent spoofing or unauthorised modifications.

Recommendations

Cryptographic hashing, tamper-resistant hardware and digital signature mechanisms should be used to verify the integrity of configuration data. Periodic integrity checks should detect unexpected modifications, and any failures should be logged for further analysis to maintain system trustworthiness.

iii. Authentication

Access to configuration functions within the QKDN manager must be restricted to verified and authorised entities.

Recommendations

The QKDN manager should adopt explicit authentication schemes, such as TLS with PKI or cryptographic tokens, to verify the identity of entities accessing configuration functions. Role-based access controls should limit privileges to authorised personnel or components, and mutual authentication should be enforced where applicable.

iv. Availability

The QKDN manager must maintain the availability of its configuration processing functions to prevent disruptions.

Recommendations

The QKDN manager should support redundant instances with automatic failover capabilities to enhance resiliency. Proactive monitoring and load balancing should maintain performance under high load conditions. Graceful degradation features should ensure that critical functions remain operational during partial system failures.

8 References

1. Recommendation ITU-T X.1710 (2020), Security framework for quantum key distribution networks.
2. Recommendation ITU-T X.1712 (2021) Corrigendum 1 (02/22), Security requirements and measures for quantum key distribution networks - key management.
3. Recommendation ITU-T X.1713 (2024), Security requirements for the protection of quantum key distribution nodes.
4. Recommendation ITU-T X.1714 (2020), Key combination and confidential key supply for quantum key distribution networks.
5. Recommendation ITU-T X.1716 (2024), Authentication and authorization in quantum key distribution network.
6. Recommendation ITU-T X.1717 (2024), Security requirements and measures for quantum key distribution network – Control and management.
7. ITU-T Technical Report (TR) FG QIT4N D2.3-part 1, Quantum key distribution network protocols: Quantum layer, 2021.
8. IMDA Reference Specification for Quantum Key Distribution Networks
9. MITRE Corporation, MITRE ATT&CK® Framework. Available at: https://attack.mitre.org/

NOTE: The above ITU-T Recommendations are referenced with permission from ITU. They may have also been partially reproduced or adapted by IMDA, and IMDA draws attention to the Notice at page 2.

Annex A

Threat Modelling and Analysis of the Trusted Node

Overview

This section provides a threat modelling analysis of the TN, grounded in the MITRE ATT&CK® framework, which offers a structured classification of adversarial tactics, techniques, and procedures. The TN is assumed to manage critical security parameters, including cryptographic key material used by various cryptographic applications.

For the purpose of this analysis, the quantum channel is excluded. It is also assumed that all classical communication interfaces are protected using mutually authenticated TLS or an equivalent secure communication protocol.

Initial Access

(Tactic: TA0001 – Initial Access)

Adversaries may attempt to gain an initial foothold in the TN through various entry points:

a. Supply Chain Compromise (T1195)

The adversary may exploit the supply chain by modifying software, firmware, or hardware prior to deployment. This includes the injection of unauthorised code into open-source dependencies, system images, or factory-installed firmware that could later facilitate access to cryptographic material.

b. Insider Access (T1078, T1565)

Privileged users or administrators may, intentionally or inadvertently, perform actions that lead to unauthorised access or compromise of sensitive assets. These actions may include unauthorised extraction, modification, or misconfiguration.

c. Physical Access to Infrastructure (T1200 / T0866)

Should an adversary obtain physical access to the protected environment, they may interface directly with equipment, management consoles, or data ports to extract or manipulate sensitive material.

d. Exploitation of External-Facing Applications (T1190)

Vulnerabilities in externally exposed services, including those using TLS, may be targeted. Even when mutual TLS is employed, improper protocol handling, deprecated cipher suites (T1557.002), flawed certificate validation, or even cryptographic side channels may be exploited. The adversary may also exploit software bugs, configuration flaws, or inadequate input validation on the lower layer mechanisms such as the Transmission Control Protocol/User Datagram Protocol/IP stack and data link interfaces.

Post-Access Activities

Following successful initial access, adversaries may undertake further actions aligned with various MITRE tactics.

a. Privilege Escalation

(Tactic: TA0004 – Privilege Escalation*; Technique: T1068)*

Exploitation of local vulnerabilities may be used to escalate privileges within the Trusted Node environment, potentially bypassing isolation or security mechanisms to access additional subsystems or data.

b. Credential Access

(Tactic: TA0006 – Credential Access; Techniques: T1552.001, T1005)

Adversaries may attempt to access cryptographic keys or authentication credentials stored in files, memory, or configuration systems, either through direct access or the use of compromised processes.

Exfiltration

(Tactic: TA0010 – Exfiltration; Techniques: T1041, T1048, T1011, T1052)

After acquiring sensitive information, adversaries may attempt to exfiltrate data from the TN via normal communication channels, alternative channels, other networks or physical media. Standard or covert (including steganographic) methods may be used to exfiltrate cryptographic key material. This includes leveraging on for e.g., HTTPS, DNS tunnelling, or encapsulation within other network protocols such as Internet Control Management Protocol, Simple Network Management Protocol, or even embedding into fields of data link frames. The leakage of cryptographic key materials may compromise the security of downstream cryptographic applications that rely on the confidentiality of the key materials.

Impact

(Tactic: TA0040 – Impact)

The adversary may take actions intended to degrade, destroy, or otherwise negatively affect the confidentiality, integrity, or availability of systems or data.

a. Data Modification

(Techniques: T1565 – Data *Manipulation; T1600 – Weaken Encryption)*

Stored cryptographic key materials and parameters may be altered to produce deterministic, weakened, or adversary-known values. These modifications may compromise the security of downstream cryptographic applications that rely on the integrity of such materials and parameters.

b. DoS

(Technique: T1499 – Endpoint DoS)

The TN externally exposed interfaces may be targeted by denial-of-service attacks, including request flooding or injection of malformed packets. Such actions may lead to service unavailability or degradation and may also be used to obscure other concurrent malicious activities.

Summary

The threat landscape for the TN spans multiple attack vectors and tactics as defined by the MITRE ATT&CK framework. While mutually authenticated TLS and restricted interfaces provide foundational security, additional layered defences are essential. These may include physical and personnel security, secure configuration management, monitoring for anomalous behaviour, and cryptographic hygiene. An effective risk mitigation approach should account for potential adversarial behaviour across the supply chain, application, network, physical, and insider domains.